

UNITED STATES DISTRICT COURT  
DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA

v.

JONATHAN MONSON,

Defendant.

\*

\*

\*

\*

Criminal No. 18-30015-MGM

\*

\*

\*

MEMORANDUM AND ORDER REGARDING MOTION TO SUPPRESS  
(Dkt. No. 52)

April 29, 2019

MASTROIANNI, U.S.D.J.

I. INTRODUCTION

Presently before the court is a Motion to Suppress filed by Jonathan Monson (“Defendant”), in which he argues that evidence from the searches of his person and his residence be suppressed. Specifically, he argues (1) the relevant search warrants were not supported by probable cause because they were based on stale information, and (2) the passcode to his cell phone was not particularized in the search warrant, was seized in violation of the Fourth Amendment, and the evidence obtained by using the passcode to facilitate a search of the cell phone should, therefore, be suppressed. A hearing was held, and for the reasons that follow, the court finds the relevant search warrants were supported by adequate cause, and suppression of the evidence obtained from the search of Defendant’s cell phone is not warranted.

## II. BACKGROUND

On March 5, 2018, Magistrate Judge Katherine A. Robertson signed three search warrants which collectively authorized the searches of Defendant; property located at 102 Morgan Street, Granby, Massachusetts (the “Subject Premises”); and two motor vehicles. (Warrants, Dkt. No. 53-1, Exs. A, B, & C.) These search warrants were all supported by an affidavit of FBI agent Ian Smythe (“Smythe”) based on an investigation of Defendant he began in June of 2017. (Warrant Aff., Dkt. No. 53-1, Ex. D.) In his affidavit, Smythe requested “authority to search the entire Subject Premises, including . . . any computer and computer media located therein where the items specified in Attachment B may be found, and to seize all items listed in Attachment B as contraband and instrumentalities, fruits, and evidence of the crime.” (*Id.* at ¶ 1.) At Attachment B, Smythe included cellular telephones on the list of items to be seized. (*Id.* at Att. B. ¶ 1.)

Smythe went on to describe “an instant messaging application for mobile devices” known as Kik Messenger (“Kik”), that “is available on most Apple iOs, Android, and Windows phone mobile operating systems free of charge.” (*Id.* at ¶ 4.) He explained how users register for unique usernames and can participate in group chats where they share photographs, videos, and links to materials from cloud-based storage services. (*Id.* at ¶¶ 5, 8.) He wrote that between June 6, 2017 and June 21, 2017, a user identified with the username “daddauluv” was observed by an FBI agent “post[ing] approximately 46 images to [a] group consistent with Child Pornography/Child Erotica.” (*Id.* at ¶ 9.)

Using information provided by Kik in response to an administrative subpoena and open-source queries, the FBI identified links between Defendant and an email account and IP address connected with the iPhone used to create the daddauluv Kik username. (*Id.* at ¶¶ 11-13.) The FBI used other commercially available information to confirm Defendant’s identity and address. (*Id.* at ¶ 14.) After connecting the Kik username daddauluv with Defendant and the address of the Subject Premises using information gathered in June of 2017, Smythe wrote that he used records searches and observations between February 21 and 27, 2018 to confirm Defendant’s continued connection to the Subject Premises. (*Id.* at ¶¶ 16-19.)

Smythe also included background information in his affidavit based on his experience with cases involving “individuals with intent to view and/or possess, collect, receive, or distribute child pornography.” (*Id.* at ¶ 20). Specifically relevant to this motion to suppress, Smythe wrote that such individuals typically retain child pornographic materials for many years and may do by storing materials in digital form. (*Id.*) Smythe also observed that those accessing or storing such materials in digital form may inadvertently leave traces of their activity that are often maintained indefinitely. (*Id.* at ¶¶ 20, 27.)

After the warrants were issued, a search of the Subject Premises was conducted. Defendant was arrested, and an Apple iPhone was found on his person. Defendant’s wife was interviewed when the search warrants were executed. In the course of that interview, she provided investigators with a passcode for Defendant’s iPhone. Without obtaining an additional warrant, investigators used that passcode to access data stored on the iPhone.

### III. STANDARD

“A warrant application must demonstrate probable cause to believe that (1) a crime has been committed—the ‘commission’ element, and (2) enumerated evidence of the offense will be found at the place searched—the so-called ‘nexus’ element.” *United States v. Dixon*, 787 F.3d 55, 59 (1st Cir. 2015) (quoting *United States v. Feliz*, 182 F.3d 82, 86 (1st Cir. 1999)). “The probable-cause nexus between enumerated evidence of the crime and the place ‘can be inferred from the type of crime, the nature of the items sought, the extent of an opportunity for concealment and normal inferences as to where a criminal would hide [evidence of a crime].” *United States v. Ribiero*, 397 F.3d 43, 48 (1st Cir. 2005). “Search warrants also have a specificity requirement, meaning ‘that warrants shall particularly describe the things to be seized,’ this requirement “prevents the seizure of one thing under a warrant describing another.” *United States v. Peake*, 804 F.3d 81, 86 (1st Cir. 2015) (quoting *Marron v. U.S.*, 275 U.S. 192, 196 (1927)).

## IV. ANALYSIS

Defendant has moved to suppress evidence obtained in the searches of his person, cell phone, computer media, and the Subject Premises because (1) the lapse of time between the Kik postings in June of 2017 and the request for the warrant in March of 2018 rendered the warrants stale and (2) the cell phone was not sufficiently delineated as an item to be searched. He also argues evidence obtained from a search of his cellphone should be suppressed because the search was effectuated using a passcode for the iPhone, but passcodes for cellphones were not among the list of items to be seized. The court first considers Defendant's argument that the warrants were stale.

The government's "affidavit supporting a search warrant must contain timely information or else it will fail." *United States v. Schaefer*, 87 F.3d 562, 568 (1st Cir. 1996). However, the court determines whether information in an affidavit is stale based on context, not a mechanical count of days. *United States v. Floyd*, 740 F.3d 22, 33-34 (1st Cir. 2014). Courts can consider a wide variety of factors when assessing whether information is timely, including "the nature and characteristics of the supposed criminal activity." *Id.* at 34 (quoting *Schaefer*, 87 F.3d at 568.) Here, aspects of the alleged criminal activity support rejecting the staleness challenge. The alleged criminal activity was the possession and dissemination of child pornographic images in digital form through an application accessed from a smartphone using a specific mobile application. It is well established, and set out in the affidavit, that individuals who create, collect, and trade child pornography are likely to hoard their collections. *United States v. Carroll*, 750 F.3d 700, 704 (7th Cir. 2014). These collections, especially when in digital form, are not perishable or consumable. Also, as discussed in the affidavit, even when erased, data about digital files is often left behind in a manner that can still be accessed. The court, therefore, finds that in the context of the specific, supposed crime, the affidavit was not stale and the warrants were supported by probable cause.

Defendant also argues the warrant did not authorize the search and seizure of Defendant's iPhone because his cell phone was not adequately delineated in the warrant. Authority to search "any computer and computer media" and to "seize all items listed in Attachment B as contraband and instrumentalities, fruits, and evidence of crime," is request in ¶ 1 of Smythe's affidavit. In

Attachment B, cellular phones are listed in the first paragraph along with computers, computer passwords, video display and storage devices, and other items that can be used to record or store images. (Warrant Aff., Dkt. No. 53-1, Ex. D. Att. B ¶ 1.) Other items listed in Attachment B include “electronic messages . . . pertaining to the possession, receipt, or distribution of child pornography;” child pornography and child erotica “[i]n any format and medium;” and “materials, in any format or medium . . . that pertain to . . . accounts with an Internet Service Provider . . . online storage or other remote computer storage.” The description of the investigation giving rise to the warrant included multiple, detailed references to cell phones, also referred to as mobile devices, and use of such devices to access the internet and share child pornography using a particular mobile application. As described in the affidavit, some of the activity was likely conducted using an iPhone connected with an IP address and email address associated with Defendant. Considering the affidavit in a common sense, rather than hypertechnical manner, it is clear that the warrant authorized the seizure and search of Defendant’s iPhone. *See Peake*, 804 F.3d at 87.

The court next turns to Defendant’s arguments regarding suppression of material obtained from the search of his iPhone. Defendant asserts the seizure of the passcode violated the specificity requirement because Attachment B to Smythe’s affidavit identified computer passwords among the items to be seized, but did not list passwords or passcodes for cellphones or smartphones. This argument is unpersuasive because it flows from the erroneous premise that his wife’s providing the passcode from her memory implicates Defendant’s Fourth Amendment protections.<sup>1</sup> Defendant’s wife was not a suspect and nothing raised by the defense or in the description of the investigators’ interview with her, during which she communicated Defendant’s iPhone passcode, indicates that she was detained or that her participation was anything other than voluntary. *U.S. v. Scott*, 270 F.3d 30, 40 (1st Cir. 2001) (“[A] suspect’s voluntary conversation with police is neither a search nor a seizure

---

<sup>1</sup> Because the court finds the passcode was not seized, it does not reach the issue of whether the reference in Attachment B to computer passwords was broad enough to include a passcode for a device like Defendant’s iPhone, which can be used both as a cellphone and to do tasks, such as accessing content on the internet, that previously required a desktop or laptop computer. To avoid a challenge of this type in the future, more care should be taken to ensure the boilerplate portions of search warrant affidavits do not include out-of-date descriptions of relevant technologies.

under the Fourth Amendment). On these facts, the passcode is appropriately treated as a voluntary communication of memory from Defendant's wife; the Fourth Amendment provides no basis for suppression.<sup>2</sup>

#### V. CONCLUSION

For the foregoing reasons, the court DENIES Defendant's Motion to Suppress Evidence (Dkt. No. 52).

It is So Ordered.

/s/ Mark G. Mastroianni  
MARK G. MASTROIANNI  
United States District Judge

---

<sup>2</sup> Defendant invites an actual/apparent authority analysis of the passcode issue but his wife only disclosed information from her memory, and based on the record before the court, appears to have done so voluntarily. The authority to search the cell phone was provided by the warrant and not, as Defendant asserts, the consent of Defendant's wife. Nor is this a situation where a third party told law enforcement where to look for tangible evidence, such as a paper notebook with passwords in it. There may be factual circumstances in which a court would need to consider whether the situation in which a third party communicated information to law enforcement necessitates an actual/apparent authority analysis. However, on the record before the court, the Fourth Amendment framing of Defendant's challenge regarding how his wife came to have and share the passcode, is inapplicable.